Together is power.

Revision E

McAfee Web Gateway 9.1.x Release Notes

Contents

What's new in the 9.1 release

Releases can introduce new features and enhancements or update platform support.

> McAfee® Web Gateway 9.1 is provided as a controlled release. For upgrade information, see the McAfee Web Gateway Installation Guide.

Kernel updated

The Linux kernel has been updated to version 4.19.

Mitigation for CPU vulnerabilities added

Vulnerabilities affecting CPUs that use hyper-threading can be mitigated by starting appliances with hyper-threading disabled.

For more information, see the *McAfee Web Gateway 9.1.x Installation Guide*.

Secure communication filtering enhanced

Regarding secure communication, filtering under the TLS 1.3 protocol is also supported for post-handshake authentication.

For more information, see the *McAfee Web Gateway 9.1.x Interface Reference Guide*.

ICMP redirection default setting changed

ICMP redirection messages are no longer accepted by default to enhance web security. In case accepting these messages is still needed, suitable entries can be made in sysctl.conf using the options provided on Web Gateway for editing system files.

For more information, see the *McAfee Web Gateway 9.1.x Product Guide*.

Transparent Bridge mode removed

Web Gateway can presently not be run as a proxy in Transparent Bridge mode. This restriction is due to a change in the product architecture.

File opening range enlarged

File opening for further inspection can also be performed now for PDF files with access restrictions.

For more information, see the *McAfee Web Gateway 9.1.x Product Guide*.

New properties

The following new properties can be used in web security rules:

- *Client.SystemInfo* provides details about the endpoint as a JSON string relayed by the MCP client over the X-SWPS-SystemInfo header.
- *SSL.Server.SkypeForBusiness.IsByPassed* checks whether the option for bypassing Skype in business traffic is enabled for HTTPS scanning.

For more information, see the *McAfee Web Gateway 9.1.x Interface Reference Guide*.

Hyper-V 2019 support

All Web Gateway versions now support use of a Windows 2019 server in a Hyper-V role.

For more information, see the *McAfee Web Gateway 9.1.x Installation Guide*.

Delivery of MMCS 2.0 supported

As the McAfee Mobile Cloud Security (MMCS) 2.0 solution is going to be applied to web security, both Web Gateway and Web Gateway Cloud Security (WGCS) will support this use of the product.

For more information, see the *McAfee Web Gateway 9.1.x Product Guide*.

Resolved issues in update 9.1.3

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

> McAfee® Web Gateway 9.1.3 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*.

Documentation revised for serial interface on WBG-5000-D and WBG-5500-D

The *McAfee Web Gateway Hardware Guide* provides information about the port assignments for network interfaces on the rear of the various Web Gateway appliance models.

You can access the RS-232 serial interface on the WBG-5000-D and WBG-5500-D appliance models using the RJ-45 connector that is located on the rear of the hardware platforms *in position 3*, as shown in the illustration below.

The assignment for this serial interface is incorrectly represented in the *McAfee Web Gateway Hardware Guide* on versions 8.1, 8.2, 9.0, and 9.1. Older document versions show this assignment correctly.

The revised illustration will also be included in the upcoming *McAfee Web Gateway 9.2 Hardware Guide*.

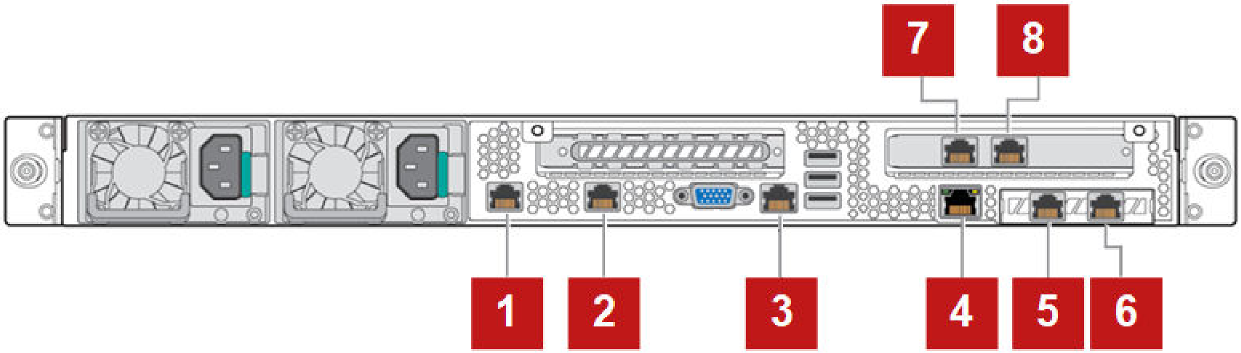

Figure 2-1 Serial interface in position 3 on rear of WBG-5000-D and WBG-5500-D

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference columns of the tables below.

Table 2-1 Network communication

Reference	Resolution
WP-2134	When a proxy is set up on Web Gateway to run in High Availability with Transparent Router mode, processing traffic under Explicit FTP works again as expected.
WP-2325	When a proxy is set up on Web Gateway to run in High Availability mode, processing web traffic is no longer slow and long running connections do not occur anymore.
WP-2495	When a Web Gateway appliance is restarted, it immediately rejoins a Windows Domain that it had been joined to before, which had been delayed due to an authentication issue.
WP-2569	The **Command.Name** property and the User-Agent header fields no longer remain empty, but are again filled with values when incoming requests are processed.
WP-2644	A package that contains the proper version of a particular OpenSSLlibrary is now used on Web Gateway after use of a different version had led to issues.

Table 2-2 Authentication

Reference	Resolution
WP-2457	When user information is retrieved for authentication under LDAPS, using a converted value as a placeholder in the search string works again as expected.

Table 2-3 Web filtering and logging

Reference	Resolution
WP-2066	When anti-malware filtering is performed, no errors originating from the AntiVirus filter module appear in the mwg-core error logs anymore, which happened before due to issues with opening archive files.
WP-2373	Auto-pushing can be performed again without problems to move access log files to an SFTP server.

Table 2-4 Vulnerabilities

Reference	Resolution
WP-2475, WP-2545, WP-2556	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2018-1311 • CVE-2019-5436 • CVE-2020-10531, CVE-2020-11100 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-5 Other

Reference	Resolution
WP-2407	Website content that users request under HTTP2 is properly displayed by Web Gateway again with no spaces left blank unintentionally anymore.
WP-2432	When a rule set for bandwidth throttling is implemented on Web Gateway, the configured speed limit for transferring data is again observed, after have been exceeded for traffic coming in from the clients.
WP-2533	The /opt partition of the appliance system is no longer filled up and the mwg-core temp file does not increase excessively anymore when large downloads are performed, which impacted performance and happened due to problems with handling size limits.

Resolved issues in update 9.1.2

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.1.1 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*.

Documentation revised for serial interface on WBG-5000-D and WBG-5500-D

The *McAfee Web Gateway Hardware Guide* provides information about the port assignments for network interfaces on the rear of the various Web Gateway appliance models.

You can access the RS-232 serial interface on the WBG-5000-D and WBG-5500-D appliance models using the RJ-45 connector that is located on the rear of the hardware platforms *in position 3*, as shown in the illustration below.

The assignment for this serial interface is incorrectly represented in the *McAfee Web Gateway Hardware Guide* on versions 8.1, 8.2, 9.0, and 9.1. Older document versions show this assignment correctly.

The revised illustration will also be included in the upcoming *McAfee Web Gateway 9.2 Hardware Guide*.

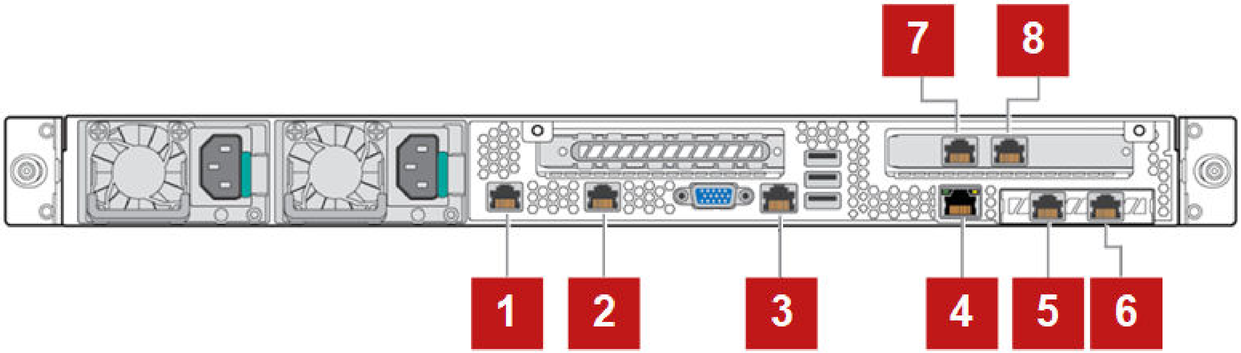

Figure 2-2 Serial interface in position 3 on rear of WBG-5000-D and WBG-5500-D

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference columns of the tables below.

Table 2-6 Network communication

Reference	Resolution
WP-2369	A value is retrieved now for the **Command.Name** property, even when a server has enforced a connection close on an SSL-secured connection and provided a different SSL certificate upon reopening the connection.
WP-2389	When Web Gateway has been configured to run as a High Availability proxy, web traffic is not forwarded to a wrong listener address anymore, which had caused faulty processing of web security rules.

Table 2-7 Web filtering and logging

Reference	Resolution
WP-2208	When Web Gateway is configured to run as an ICAP server, slowness in scanning files received for malware detection due to the file opening that is performed by the Composite Opener does no longer occur.
WP-2266	When DLP filtering is applied to web traffic going on under ICAP, files with embedded objects sent in response to a download request are now forwarded properly, not using a REQMOD request anymore, which had led to an ICAP client error.
WP-2325	A general slowness in browsing observed on Web Gateway clients has been fixed and does no longer occur.
WP-2441	When customer-subscribed lists are downloaded, the option for ignoring certificate warnings is recognized again, which had temporarily not worked and caused downloads to fail.

Resolved issues in update 9.1.1

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.1.1 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*.

Documentation revised for serial interface on WBG-5000-D and WBG-5500-D

The *McAfee Web Gateway Hardware Guide* provides information about the port assignments for network interfaces on the rear of the various Web Gateway appliance models.

You can access the RS-232 serial interface on the WBG-5000-D and WBG-5500-D appliance models using the RJ-45 connector that is located on the rear of the hardware platforms *in position 3*, as shown in the illustration below.

The assignment for this serial interface is incorrectly represented in the *McAfee Web Gateway Hardware Guide* on versions 8.1, 8.2, 9.0, and 9.1. Older document versions show this assignment correctly.

The revised illustration will also be included in the upcoming *McAfee Web Gateway 9.2 Hardware Guide*.

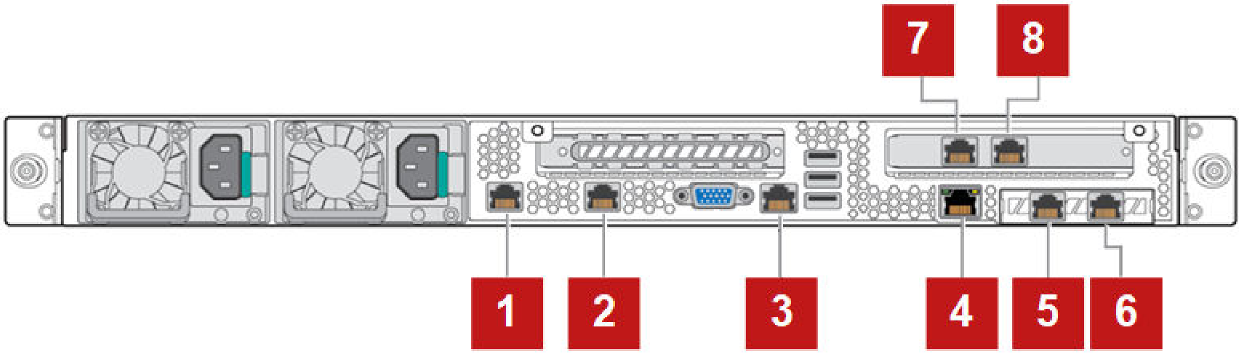

Figure 2-3 Serial interface in position 3 on rear of WBG-5000-D and WBG-5500-D

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference columns of the tables below.

Table 2-8 Network communication

Reference	Resolution
WP-2300	When decrypted traffic is monitored, source ports are no longer set to zero, but retain their original values.

Table 2-9 Web filtering

Reference	Resolution
WP-2282	A certificate chain for the user interface that could not be imported is made available again for importing when handling SSL-secured traffic.

Table 2-10 Vulnerabilities

Reference	Resolution
WP-2299, WP-2323, WP-2348	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2019-1551 • CVE-2019-17569 • CVE-2020-1935, CVE-2020-1938 This vulnerability was already mitigated in version 9.1: • CVE-2019-11135 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in the 9.1 release

This release resolves known issues.

JIRA numbers are provided in the reference columns of the tables below.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

Table 2-11 Network communication

Reference	Resolution
WP-1843	The user interface no longer disappears intermittently when Web Gateway is running as a High Availability proxy.
WP-2049	The X-Forwarded-For Header is filled with the value for the IP address of the client that sent a particular request when Web Gateway is running as a High Availability proxy, whereas the field had previously been filled with a virtual address.
WP-2077	When multiple port redirects are created for Web Gateway to run as a High Availability proxy in Transparent Router mode, not only the one that was created last, but all of them appear in haproxy.cfg.
WP-2078	When Web Gateway runs as a High Availability proxy in Transparent Router mode, creating a portredirect with a space before the port number no longer causes the proxy to fail.
WP-2112	When Web Gateway runs as a proxy in Transparent Router mode, HTTP and FTP traffic going to the ports configured for the IP addresses of inbound and outbound interfaces is again picked up and redirected to the proxy port as laid down in the iptables rules, regardless of whether a VRRP interface is involved or not..
WP-2137	When Web Gateway runs as a High Availability proxy, the default timeout for client and server responses, which is set in /etc/haproxy/haproxy.cfg, has been increased to avoid frequent signing on and off.
WP-2141	Socks connections work again when Web Gateway is running as a High Availability proxy using virtual IP addresses.
WP-2143	When uploading a file from a client to a server over an active or passive FTP connection, the Proxy-Protocol header gets no longer prefixed to the content data.

Table 2-11 Network communication *(continued)*

Reference	Resolution
WP-2147	When Web Gateway runs in Transparent Bridge mode, enabling IP spoofing does not prevent HTTPS connections from working anymore. This network mode is not available for this release, but will be reintroduced later on.
WP-2242	The core and coordinator processes no longer fail, which had happened due to operations being called on Web Gateway while referring to a pointer with null value in Open SSL.

Table 2-12 Web filtering and logging

Reference	Resolution
WP-1593	When bonded interfaces are in use on Web Gateway, IP addresses are again included in the names of the log files that record this use.
WP-1829	The haproxy log is no longer filled up with error messages after an issue with handling connections coming in at server downtime has been fixed. Performing log file rotation upon reaching a daily size limit is now sufficient to avoid an excessive log volume.
WP-2139	Processing Incoming requests on Web Gateway runs smoothly again after an issue with handling files compressed under gzip has been resolved.
WP-2205	A temporary file in the /opt partition on Web Gateway no longer increases until the partition is filled out, which had happened when the Stream Detector did not recognize a live stream that had been left open over several days, but tried to download and save it.

Table 2-13 Vulnerabilities

Reference	Resolution
WP-1585, WP-1825, WP-1950, WP-2024, WP-2111, WP-2135, WP-2145 , WP-2299	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2018-3620, CVE-2018-5741 • CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-19519 • CVE-2019-1125, CVE-2019-2975 • CVE-2019-11091, CVE-2019-11135, CVE-2019-11729, CVE-2019-11745, CVE-2019-12418, CVE-2019-17563 For more information about each CVE and its impact, see the Red Hat CVE portal.

Table 2-14 Other

Reference	Resolution
WP-2110	An issue that led to a segmentation fault and a failure of the core process, which caused Web Gateway to terminate with term signal 11, does not occur anymore.

Rating for update 9.1.3

The rating defines the urgency for installing this update.

Recommended

Mandatory	Critical	High Priority	**Recommended**

- Recommended for all environments. Apply this update at the earliest convenience.
- Not applicable to hotfixes, because a hotfix is only created in response to a business-impacting issue.
- An update that resolves non-severe issues or improves product quality is considered as recommended.

For more information, see KB51560.

Together is power.